### Record of Release

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Modified By</th>
<th>Reviewed By</th>
<th>Authorized By</th>
<th>Release Date</th>
<th>Modifications Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Manish Ugave</td>
<td>Saigiri Ella</td>
<td>Sagar Pise</td>
<td>8-Nov-2017</td>
<td>Initial Release</td>
</tr>
<tr>
<td></td>
<td>Hariharan MV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

1.0 iDiscover Basics ................................................................. 3
  1.1 Overview ........................................................................... 3
  1.2 Highlights ........................................................................ 3
  1.3 iDiscover Block Diagram ..................................................... 4
    iDiscover comprises of following building blocks: ...................... 5
  1.4 System Requirements .......................................................... 6

2.0 Using iDiscover ................................................................. 6
  2.1 How to start iDiscover: .......................................................... 6
  2.2 Configuring Database connections: ......................................... 6
  2.2 iDiscover functionalities ....................................................... 9
  2.3 Sensitive Data Discovery ...................................................... 10
    2.3.1 Map for country selection ............................................... 10
    2.3.2 Job Name: .................................................................. 10
    2.3.3 Agent Details: ............................................................... 10
    2.3.4 Sensitive Fields: ........................................................... 12
    2.3.5 File Configuration: ....................................................... 13
    2.3.6 Global Configuration: .................................................... 14
    2.3.7 Trigger Execution Options: ............................................. 19
    2.3.8 Save Job Details Option: ............................................... 19
    2.3.9 File Category: ............................................................... 19
  2.3 iDiscover Data Breach: ....................................................... 19
  2.4 iDiscover Reports: ............................................................. 22
  2.5 iDiscover Admin Functionality: ............................................. 24
    Admin have the right to Create User, Delete Existing User and change password .................................................. 24
  2.7 Change Password: ............................................................. 27

Contact Us: ............................................................................ 28
1.0 iDiscover Basics

1.1 Overview

LTI’s iDiscover is an automated solution that simplifies your route to GDPR compliance. The very first step in any compliance is to identify sensitive data fields in given application or database landscape along with its dependent data points. iDiscover does this in an automated way, by scanning entire data systems configured in tool and generates detailed reports.

iDiscover helps to configure and scan multiple databases/Files to identify sensitive fields that contain any structured, unstructured, PII, PCI and PHI data. It provides both flexibility and country-specific customization to select, add and execute algorithms to discover sensitive data. Reports generated have information of all sensitive columns and its dependent entities. Tool not only looks for field names, to recognize particular column as sensitive column, but it also looks at actual data values.

1.2 Highlights

- Country specific rules / algorithms
- Automated GDPR Tool empowering Data Protection Officer
- Historical tracking of sensitive data, periodic changes in data & location
- Early & continuous data protection
1.3 iDiscover Block Diagram

iDiscover block diagram is shown below,
**iDiscover comprises of following building blocks:**

1. **Communication Manager:**
   Communication Manager is responsible for reading data from variety of data sources such as RDBMS, Flat files, Excel files and Word documents. Federal communication API’s have been developed in this layer which takes care of seamless connection to given data source.

2. **Configuration Manager:**
   iDiscover is highly configurable solution in term of various databases, file formats, features and reports. Configuration Manager takes care of creating, updating and deleting such configurations.

3. **Core Engine**
   Core Engines consists of various data algorithms which are developed in modular way. This component contains data discovery algorithms specifically developed by understanding GDPR sensitive data requirements.
   Data search is one of the important activity required in entire GDPR process and aspects such as data portability & right to forget. Data Search Engine looks after this aspects.
   It also have algorithms, which are used to identify sensitive data differences across consecutive releases and builds.

4. **Report Manager:**
Report Manager is responsible for generating iDiscover reports by taking various sensitive data information from core engine. Separate reports are generated for sensitive data discovery, data search and data breach. Along with sensitive data information, report also highlights information about dependant data points based on physical referential integrity.

1.4 System Requirements

- Windows OS
- 3 GHz CPU
- 4 GB RAM
- JRE 1.7 (For Tomcat)
- JRE 1.8 (For ActiveMQ)
- Microsoft Office
- Windows OS
- Database Server SQL Server 2008 or MY SQL Server version 5.5: Read Access is required (Database which tool is scanning).
- Adobe Reader 11.0

2.0 Using iDiscover

2.1 How to start iDiscover:

Please refer Installation guide for Agent and Server.

2.2 Configuring Database connections:

- After successful login on iDiscover tool, click on connection menu option.
- Database configuration
  - In Database Configuration you have to enter below details:
    - ID
    - Vendor name
    - Application Server
    - Connection Name
    - Database Name
    - Username & Password
    - Windows Authentication
    - Port No.
Connection Using database Configuration shown below

<table>
<thead>
<tr>
<th>ID</th>
<th>Vendor</th>
<th>Application Server</th>
<th>Connection Name</th>
<th>Database Name</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>SQLServer</td>
<td>172.20.40.76</td>
<td>compliance_portal</td>
<td>Compliance_portal</td>
<td>12</td>
</tr>
</tbody>
</table>

- **SAP BW Configuration:**
  - In SAP BW Configuration you have to enter below details:
    - ID
    - Vendor name
    - Application Server
    - Connection Name
    - Database Name
    - username & Password
    - Windows Authentication
    - Port No.

Connection Using SAP BW Configuration shown below
• **Database Table Mapping**: To upload table List file related to SAP Connection details

  ➢ In Database Table Mapping you have to enter below details:
  
  • Job Name
  • Machine Name
  • Connection Name
  • Upload List of Table file: browse table list file
Database Table Mapping shown below

On successful addition of database configuration you can move to Sensitive data Discovery.

2.2 iDiscover functionalities

1. **Sensitive Data Discovery**
   Scan sensitive data fields in database and files (Structured and Unstructured) and gives result in PDF reports and HTML Reports contains sensitive data field, and user access permission (applicable for database only).

2. **Data Breach**
   This functionality compares two consecutive reports and give the difference in form of graphs containing matched, unmatched and newly added data differences.
2.3 Sensitive Data Discovery

Sensitive Data Discovery screen shown below:

iDiscover has following main components:

2.3.1 Map for country selection:

User can select any country from the map to scan the fields particular to that selected country.

2.3.2 Job Name:

Here you can select existing or saved job for sensitive data discovery created by that user.
By clicking on (+) button you can create new job.
User can add one or more path, one or more Database connection as part of single job and scan in a single go.

2.3.3 Agent Details:

Here you have to select agent for data discovery. You can also see the status of agent like
- Online-Executing
- Offline
- Online Available

Agent Details screen shown below:
### Job Name

TestRun1

<table>
<thead>
<tr>
<th>Select</th>
<th>Status</th>
<th>Name</th>
<th>IP</th>
<th>File Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Online</td>
<td>INFPU08531</td>
<td>172.20.89.118</td>
<td>D:\Discover Agent\Dis</td>
</tr>
</tbody>
</table>

**Sensitive Fields**

**File Configuration**

**Global Configuration**

**Save Job Details**
**File Configuration** to add path of folder for scanning. We can add or delete any path for particular execution.

**DB Configuration** to add Connection (Created in connection Tab) for scan. We can add or delete any connection for particular execution.

### 2.3.4 Sensitive Fields:

Under sensitive field user need to select fields.

Fields are fetched based on country selection and this contains 68 fields identified as PCI, PHI, PII.

Sensitive field screen shown below:
2.3.5 File Configuration:

User need to specify the types of file to be scanned. User can select multiple file types and scan in a single execution. Types of files that can be scanned.

1. **PowerPoint** - PPT/PPTX
2. **PDF**
3. **Excel** - XLSX /XLS
4. **Images** – GIF, JPEG, BMP, PNG, JPG
5. **Word documents** - DOC/DOCX
6. **Semi-Structured Flat File** - Files like CSV, PSV
   a. User can mention the delimiter in the delimiter text box.
   
   Example: for csv user can mention delimiter as ‘,’.
7. **Unstructured Flat File** - TXT, DAT.
   a. User can mention the file extension in the Unstructured File Type text box.
   
   Example: for txt user can mention .txt.

Created Date/Modified Date:

User can specify the filter criterion to scan the files. There are three types of criteria.

1. **All Files** - By default all files is selected and all the files in the configured path will be scanned by iDiscover.
2. **Modified Date** - iDiscover scans only the files which matches the modified date of the file.
3. **Created Date** - iDiscover scans only the files which matches the created date of the file.

File Configuration screen shown below:
2.3.6 Global Configuration:

In global configuration user need to provide below details for Files/Database:

- **Sensitive Data limit for File/database = 100**

Sensitive data limit is configuration for number of rows (starts with initial row) need to fetch from each table of searching database. Rang: based on number of row has to work on.

- **Sensitivity Threshold (%) = 100**
Threshold value defines the accuracy of sensitive data matched in database or files, on the basis of this threshold value tool will decide the sensitive data has to be included in the report or not (i.e. density of sensitive data found). Value range: 1 - 100

Show Permission: Yes/No

If YES user will get permissions (Insert, Update and Delete) in reports of each column in database.

Thread:

You need to specify number of thread for parallel execution.

Meta Info Scan:

You need to select High or No for Meta Info Scanning type.

Meta Info File and Category File:

Here you need to upload Match_Names.txt and fields.txt.

Match_Names.txt contains sensitive field’s column names with their Meta information (alias names).

If data in a particular column is null/blank then tool will refer MatchNames.txt as based on column name iDiscover will take it as sensitive data. User have to upload this Meta information file.
Screen shot of a sample Meta information file:

Fields.txt contains categorization for each sensitive fields.

Out of 5 categories Confidential-Personal, Confidential-Sensitive, Public, Private & Internal,

iDiscover will tag the input file based on sensitive fields identified.
Screen shot of a sample field Category file:

```
CPR number:Confidential-Personal
SSN:Confidential-Personal
Personal Identity number:Confidential-Personal
Personal Identity Code:Confidential-Personal
Norwegian ID number:Confidential-Personal
Passport number:Confidential-Personal
Date of birth:Confidential-Personal
Full name:Confidential-Personal
First name:Confidential-Personal
Last name:Confidential-Personal
Home address/Street Name:Confidential-Personal
State:Confidential-Personal
City:Confidential-Personal
Postal code:Confidential-Personal
Postcode1:Confidential-Personal
Postcode2:Confidential-Personal
Email address:Confidential-Personal
Telephone number:Confidential-Personal
Mobile number:Confidential-Personal
Fax Number:Confidential-Personal
Old claim ref number:Confidential-Personal
Insurer claim no:Confidential-Personal
Gender:Confidential-Personal
Nationality:Confidential-Personal
Credit card number:Confidential-Sensitive
Debit card number:Confidential-Sensitive
Vehicle Identification Number:Confidential-Personal
Medical Insurance Number:Confidential-Personal
Driver's license number:Confidential-Personal
Country:Public
Precinct:Confidential-Personal
Bank Account number:Confidential-Personal
Certificate/license numbers:Internal
```
Screen for global configuration shown below:

### Files

<table>
<thead>
<tr>
<th>Sensitive Data Limit</th>
<th>10000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold (%)</td>
<td>0.0001</td>
</tr>
</tbody>
</table>

### Database

<table>
<thead>
<tr>
<th>Sensitive Data Limit</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold (%)</td>
<td>10</td>
</tr>
</tbody>
</table>

| Show Permission      | NO    |

### General

<table>
<thead>
<tr>
<th>Threads</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meta Info Scan</td>
<td>High</td>
</tr>
</tbody>
</table>

### Meta Info File

- **Choose File**
  - No file chosen
- **Upload File**
  - Match_Names.txt

### Category File

- **Choose File**
  - No file chosen
- **Upload File**
  - fields.txt
2.3.7 **Trigger Execution Options:**

Using trigger execution option you can start scanning data or files at agent for the selected job and configuration.

2.3.8 **Save Job Details Option:**

Here user can save job details for future execution.

2.3.9 **File Category:**

After execution, files in which sensitive fields are found is tagged with file category by adding custom property.

**Custom property name:** “iDiscover Category”

Value is added in [MOG/CATEGORY] format and also if category contains “-” it is replaced with “/”.

- Ex. 1. If file category found is “Private”, Custom property value will be [MOG/Private].
- Ex. 2. If file category found is “Confidential-Sensitive”, Custom property value will be [MOG/Confidential/Sensitive].

2.4 **iDiscover Data Breach:**

This functionality compares two consecutive reports and give the difference in form of pdf reports and Graphs contains unmatched and newly added data differences.

**Note:** Graph contains consecutive list of builds and total difference between this builds. Builds are Build Numbers is generated at the time, when 2 consecutive reports (for DB) or job(For Files/DB) which has some difference in the current and last execution.

There are 2 graphs generated in data breach, first is for the list of consecutive builds and total difference (fig 2.4.1). Second is for the particular build point, shows the unmatched and newly added data and total difference (fig 2.4.2).
Screen for Data breach Menu show below:
There are two sub menus for Data Breach:

1. **Data Breach File**:

   **Job Name:**
   
   ![Job Name: Testjob](image1)

   **Machine:**
   
   ![Machine: 172.20.89.47](image2)

   **Start Time:** 2017/11/01 18:08

   **End Time:** 2017/11/07 18:08

   ![Analyze](image3)

In Data Breach file user can analyze unmatched and newly added data differences from the report generated by comparing a job for its current and previous execution based on job name selection and machine for particular time interval.

Note- Analysis is done on the particular job and machine
2. Data Breach Database:

In Data Breach Database user can analyze unmatched and newly added data differences from the report generated by comparing two consecutive reports based on the job name, machine and connection for particular time period.

Note- Analysis is done on the particular job, machine and connection

2.5 iDiscover Reports:

Here user can view reports graphically for File and Database.
Graphs are generated based on job name, timestamp, database (in case of database reports) and machine IP.
Screens for File and Database report generation form shown below:
There are two graphs generated:

1. **Field Distribution graph:** This graph shows the count of sensitive fields found and not found.

2. **Field Concentration graph:** This graph shows concentration of each field identified in database/files that is, how many times that field has been identified in a particular table or file.

For each field we will get the details regarding path of folder and file name in which sensitive field is identified. In case of database we will get the details like table name, column name, key type and reference table name.

### 2.6 iDiscover Admin Functionality:

Admin have the right to Create User, Delete Existing User and change password

1. **Create User** - New user must be created for the first time only by the admin after installation. Admin can create any number of users.
Create User screen shown below:
2. **Delete User** - Admin has a privilege to delete an existing user for which he has to mention the username to be deleted and admin password.

Delete Existing user screen shown below:
2.7 Change Password:

Both User and Admin can change their respective passwords by giving their current password. To change password the user or admin first need to login using that user name for which he/she thinks the password needs to be changed.
Contact Us:

For any queries or suggestions, please get in touch:

TCGTeam@Lntinfotech.com